Final Technical Report
Contract Number
Delivery Order

CS98 – J10.1
DAAH01-97-D-R005
#001

# Computer Network Analysis and Implementation

## Final Report
**October 1998**


Prepared By:

Dr. James D. Johannes
Mr. Tim Lewis
Mr. Kyle Hoover
Mr. Andrew Fanning
Mr. Chad Williams
Ms. Marsha Robinson
Mr. Roland Troland






The University of Alabama in Huntsville
Huntsville, Alabama 35899


Prepared for Software Engineering Directorate

dh

PLEASE CHECK THE APPROPRIATE BLOCK BELOW

DAO# _____

☐ _____ copies are being forwarded. Indicate whether Statement A, B, C, D, E, F, or X applies.

☒ DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

☐ DISTRIBUTION STATEMENT B:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES ONLY; (indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT C:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTS (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT D:
DISTRIBUTION AUTHORIZED TO DoD AND U.S. DoD CONTRACTORS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT E:
DISTRIBUTION AUTHORIZED TO DoD COMPONENTS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT F:
FUTHER DISSEMINATION ONLY AS DIRECTED BY (Indicate Controlling DoD Office and Date) or HIGHER DoD AUTHORITY.

☐ DISTRIBUTION STATEMENT X:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND PRIVATE INDIVIDUALS OR ENTERPRISES ELIGIBLE TO OBTAIN EXPORT-CONTROLLED TECHNICAL DATA IN ACCORDANCE WITH DoD DIRECTIVE 5230.25. WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE, 6 Nov 1984 (indicate date of determination). CONTROLLING DoD OFFICE IS (Indicate Controlling DoD Office).

☐ This document was previously forwarded to DTIC on _____ (date) and the AD number is _____.

☐ In accordance with provisions of DoD instructions. The document requested is not supplied because:

☐ It will be published at a later date. (Enter approximate date, if known).

☐ Other. (Give Reason)

**DoD Directive 5230.24, "Distribution Statements on Technical Documents," 18 Mar 87, contains seven distribution statements, as described briefly above. Technical Documents must be assigned distribution statements.**

JAMES T. JOHANNES
**Print or Type Name**

J. T. Johannes
**Authorized Signature/Date**

890-6255
**Telephone Number**

## FORWARD

The University of Alabama in Huntsville appreciates the opportunity to support the development and expansion of the local area network (LAN) for the U.S Army's Software Engineering Directorate (SED). Our involvement in the earlier development of the LAN provides us with a unique insight into the SED LAN and its users. The team assembled to work on this effort was thus able to provide a historical perspective on technology growth that few others could have.

Part of the analysis of a computer network like that at SED involves planning for long term use. This includes planning for new equipment, growth in services, and smooth transitions to new technologies. Planning for new technologies involves ensuring that they can be migrated from the center of the network (high-speed communication between parts of the network) to end user technology (connection to the desktop) as the core of the network is upgraded over time. This process is not unlike the strategy auto manufacturers use, adding a new top of the line model every few years, dropping the lowest end model at the same time. Our recommendations for high-speed networking stem from an analysis of the long-term growth potential of new technologies and the (in) appropriateness of upgrading end user connectivity in the short term.

SED Network Support Team

Dr. James D. Johannes
Tim Lewis
Kyle Hoover
Andrew Fanning
Chad Williams
Marsha Robinson
Ronald Trolard

# TABLE OF CONTENTS

# 1.0 INTRODUCTION

This is the final report for DAAH01-97-D-R005 Delivery Order (D.O.) 1, "Computer Network Analysis and Implementation." As such, it represents the collective effort of seven UAH employees, together called the 'SED Support Center Team,' or simply the 'Support Center', over the course of eleven months.

This report details the activities related to the various tasks in the D.O. and is arranged by task within section 2. Section 3 summarizes the activities and recommendations of the Support Center. A list of items purchased on this D.O. is included in appendix A.

# 2.0 Activity Reports

The following sections cover the various tasks in the D.O. The relevant activities for each item are summarized within the appropriate section. Each section opens with the text from the Statement of Work (SOW), detailing the requirements for that particular area of effort; this provides the context for the activities performed.

## 2.1 Electronic Mail Systems

*Research architectural and equipment issues related to implementation of a generalized organizational E-mail backbone and delivery system given the current SED E-mail relays and transfer agents. Include a determination of the impact of implementing Defense Messaging System (DMS) compliant system for computer network systems. Implement and test candidate solutions.*

Microsoft Exchange is the primary E-mail system in use at SED. The SED Exchange server now has over three hundred users, and handles the load well. The process of moving the entire user community of the SED continues, though at a slower pace than recently because most users are already migrated. On average, a new user is added to the server every day, some from other SED E-mail systems, but mostly users that have just arrived at SED. The SED user community continues to grow, and much larger growth is anticipated in the future due to a new building being added to the SED complex. Several upgrades have been performed on the Exchange server during this D.O. in the continuing effort to achieve greater connectivity and capability for the Exchange users. The following sections describe the research and upgrades performed on the Exchange system. The primary research effort was toward adding connectivity to the Exchange system.

1) *Integration of the SED address list with the larger Redstone Arsenal address list.*

Like most modern messaging systems, the Exchange E-mail system has a built-in address book that allows users to find other users by name (or other information) instead of by their E-mail address, which may be unpredictable. The AMCOM Corporate Information Center (CIC) runs a number of E-mail servers for different organizations on the Redstone Arsenal. Most of these servers are cc:Mail servers, but integrated with the cc:Mail are a number of Exchange servers. The users at the SED want connectivity to the address books on the CIC mail servers. It was hoped that our Exchange server could be linked to one of the CIC Exchange servers and share address lists.

Linking Exchange servers together is very difficult unless the linking was planned when the servers were originally configured. Each Exchange server keeps its user database in a hierarchical format. At the top level of the hierarchy is the organization, and under that are various "sites" where E-mail servers are

located. At each site are servers, and at each server are a number of user mailboxes and other end nodes for the hierarchy. The problem with linking two Exchange servers occurs when the server organization names do not match. It is not possible to link servers with different organization names. At this time, it is also impossible to change an organization name on a server without completely re-installing the server software and re-initializing the entire user database. Unfortunately, the SED Exchange server has a different organization name than the CIC Exchange server. The network support team spent significant time searching for ways to integrate the SED server with CIC and found there is no practical way to do it at the moment. Microsoft has announced a utility for Exchange that will allow the organization name to be changed easily, but the release date of that tool is not set. Until the tool is released, the SED server cannot be integrated with that of CIC.

In the meantime, some other preliminary steps were taken towards this integration. First, the E-mail addressing convention used by the Redstone Arsenal was adopted by the SED so that when the eventual linking occurs, the addressing conventions will match. This convention was adopted for new users in the SED database after it was announced, but there were numerous exceptions from earlier users that had to be modified. Second, the SED Exchange Server was upgraded to version 5.5 from 5.0. This was done for several reasons, one of which was to ensure complete compatibility with the CIC servers.

2) *Integration of the Exchange address list with other SED databases.*

In addition to the need to integrate Exchange with the CIC E-mail server, there is a significant need to integrate Exchange with the local database systems at SED. The central database for SED is kept in an Oracle database. The Oracle database contains latest directory information for all the people who work at SED. Included in this database is the E-mail address of each person, their room number, phone number, project name and other pertinent information. The Exchange database tracks some of the same information independently. The authoritative source for the project information is the Oracle database, while the authoritative source for a user's E-mail address is the Exchange server. This means that the Oracle database must periodically be updated with E-mail addresses from the Exchange database, and the Exchange database must be updated with other information from Oracle. Several approaches were taken to solving these problems.

The first solution was to port data from Oracle to the Exchange server using comma separated value (CSV) text files. An Oracle script was written that would export all the relevant data from the Oracle server to a CSV file that Exchange could then import. The E-mail address data from the Exchange server was entered in the Oracle database by hand, because the number of changes was relatively small after the initial data entry. However, the SED is quickly outgrowing this solution. The CSV files generated by the Oracle script worked well for small numbers of Exchange users and large numbers of "external" users (users not on the Exchange system.) But as SED has been migrated to the Exchange server, the usefulness of the CSV files has diminished. Also, with the

increased number of users, it is becoming impractical to update the Oracle E-mail addresses by hand.

A couple of new solutions to the database synchronization problem are currently being researched. A new script file has been written to deal with the CSV files that will help us synchronize the E-mail addresses on the Oracle server. For sending the rest of the information to the Exchange server, Microsoft's Visual Basic scripting, and the enhanced LDAP (Lightweight Directory Access Protocol) features that came with the Exchange 5.5 upgrade are being researched. Visual Basic has internal hooks into the Exchange system that allow it to operate on Exchange objects (such as user's accounts and mailboxes) directly, and it can also interface directly with the Oracle database system. This technology allows the writing of scripts that will more effectively synchronize the data. Visual Basic hooks to other systems are complex however, and there is still much research required in this area. The LDAP solution is not quite as neat as the VB scripting solution, as it would still require CSV files to be passed between servers, but the amount of information available to LDAP clients is much greater than we can extract with the simplistic Exchange export features. This method of synchronizing the database systems has potential, and needs to be researched more thoroughly.

3) *Groupware Features*

Recently, a new requirement for the Exchange system has surfaced at the SED. Many customers at SED process large numbers of government forms. There is a specific workflow associated with each form, and a significant amount of effort goes into tracking a form as it moves from person to person throughout the building. Also, much of the form data has to be re-entered manually when it leaves one computer system and enters another. Many SED customers would profit if they could fill out their forms on-line and route them through the E-mail system. It would help them even more if this form data could be moved from the E-mail system into other government database systems automatically. The Microsoft Exchange system has a built-in form-handling feature. Furthermore, many pre-programmed government forms already exist for the Exchange system. Routing forms and uploading data to other systems is a little more complex, and further research is needed in this area, but Visual Basic scripting is one possible solution.

4) *The Impact of DMS*

The Defense Messaging System (DMS) would dramatically impact any corporate E-mail system if it were implemented today. However, the requirements and standards for DMS are still fluctuating significantly, and thus to determine exactly how DMS would impact SED is nearly impossible at the present time. There is, however, a DMS compliant version of Microsoft Exchange available. SED is not presently running this version because (1) it lacks some features that the current server supports, (2) it is significantly more expensive than the current system, and (3) it would require that specialized user authentication hardware be added to many of the computers in SED. When SED

is required to migrate to DMS, the impact will be minimized by the fact that the current mail server in use at the SED is Exchange.

**Future Plans**

The following is a list of notable events and future plans that concern the Exchange server:

- The Y2K patch for Windows NT was installed on the SED Exchange Server, making the system 100% Y2K compliant.

- Recently, Microsoft has released the Outlook '98 Exchange client software. This software comes pre-installed on many new users' machines, while other users are being upgraded to this client. The only caveat is that Outlook '98 is much larger and more demanding on the computer's processor than the old Exchange client, and some users' computers cannot support it.

- The process of moving users from other E-mail servers to the Exchange server has been going very well, as mentioned before. Both the C3I cc:Mail system and the UAV E-mail server have transferred all users to the main SED Exchange Server. Originally these servers supported between 150 and 200 users, so this move is considered a significant milestone.

- It is anticipated that the Exchange server will be moving to a new platform in the near future. The new platform will be a faster dual-processor Alpha server. The current Alpha server will then be used for a backup server for the Exchange system. This will give the SED 100% redundancy on the E-Mail system. Clustering technology is being researched to provide further system reliability.

## 2.2 WWW Architecture

*Research architectural, software, and equipment issues related to the implementation of multiple World Wide Web (WWW) home pages. An architectural/security model shall be developed to address provisions for controlling access to some information while making other information publicly available. Implement and test candidate solutions.*

The Software Engineering Directorate maintains multiple WWW sites, including one "public access" site and various Intranet sites, designed for internal use only. The public access web site is an information site only; it describes the function and activities at the Software Engineering Directorate, and provides command structure and contact information for SED. There is also a main Intranet site, internally called Infocenter, which serves as an internal information resource for users at SED. From this site users can access various command documents such as SEPH (Software Engineering Process Handbook) or other guidelines used by the SED command for software engineering. Users are able to receive information on various services provided to them via the SED network, such as E-mail services or remote dial-in services, and links to the SED

internal periodical. There are also links to other Intranet sites that tie in to an internal Oracle database. This database maintains information useful to the SED community, such as a telephone directory, equipment ownership database, and conference room scheduling system.

The Web server used is Purveyor for OpenVMS. Earlier trials were done using Netscape Enterprise Server 3.0 for NT. This software package proved to be very versatile and robust. However, it was unable to tie in as cleanly to the Oracle database functioning on the OpenVMS system already in place. Also, OpenVMS is a much tighter system in the security realm. As a result, a decision was made to use Purveyor for the time being. It runs on the same system as the Oracle database and is able to use a single user authentication method for the closed database systems. Netscape has promised a future release of its web server for OpenVMS. When that version arrives, the issue of using Netscape Enterprise Server will be revisited and tested for the same capabilities.

Security is handled by rules based security on the web server, securing access by Internet location. Specifically, on the Internet side (public domain), all users are allowed read access to the server pages. Only specific internal users are allowed access to modify any pages, and this is prohibited via a web browser. All internal web sites are prohibited access by any users outside the SED community via rules based security. Maintaining all information on the OpenVMS server greatly reduces the risk of tampering or "hacking" of any Internet or Intranet sites at SED.

Content on the Intranet site is a constant work in progress. As new services or new notices become available or necessary, a decision is made and content is altered to make them available to the SED community.

## 2.3 Computer Network Monitoring

*Research solutions to provide for computer network monitoring. This will include error detection/recovery and will consider computer network security. Implement and test candidate solutions.*

In general, network management takes two very different forms. One class of network management products is aimed at the physical network: the network cables, bridges, routers, terminal servers, hubs, and other network hardware. Another class of network management products deals with the management of the end nodes of the network: the computers, printers, and other user-interface devices attached to the network.

ClearVISN, a management utility created by Digital Equipment Corporation, gives the ability to manage all network equipment via a graphical utility from a single workstation. ClearVISN is a policy based network management product which allows SNMP configuration for all DEC hub based products, including switches and VLAN (virtual LAN) management. This also includes firmware upgrades to almost all modules.

The network analyzer Network General Sniffer® has proved to be a valuable tool in network monitoring. The Sniffer® provides full OSI protocol analysis for approximately 200 different network protocols, including all layers from the network layer to the application layer. The Sniffer is also valuable for troubleshooting network-related errors, both on the physical level and the protocol level. We currently are using two Network General Sniffers: an FDDI version and an Ethernet version. This capability allows monitoring of all facets of traffic throughout the SED network, either on the backbone or on individual workgroup segments. Expansion plans for the SED network include upgrading to Fast Ethernet to the desktop. When this happens there will be no monitoring capability for the Fast Ethernet because none of the current Sniffer products can monitor at Fast Ethernet speed. There is a new product available which allows sniffing of Ethernet, Fast Ethernet, and various other protocols, from the same company that created the Ethernet and FDDI version, although this version is based on Windows instead of DOS. When a transition is made to include Fast Ethernet to all desktops, a recommendation will be made to include this latest version of Sniffer in the Support Team's tool chest.

Right now security is being handled on a case-by-case basis, including searching for invalid network addresses and manually analyzing log files on the various servers for evidence of possible tampering. Further research is necessary to determine an effective method of organizing these log files. A strong possibility is Seagate's Crystal Reports. This package allows custom configuration of reports that will read these log files and organize them into one easily read report.

Towards the end of this D.O., an Army Regulation was released to the Support Team that outlined what security methods the group is allowed to use. Army regulation AR 380-19 specifies that only C2 authorized products specifically designated by the Army are allowed in Army installations for security scanning. The Army researched a product called ISS SPINT, which gives the ability to scan all machines in a network for any security hazards that may be open to intrusion from outside the network. This product will run a full scan on all ports on a workstation and report on any possible hazards. For Windows based workstations, this is the only authorized tool for system security monitoring. There is also a version for Unix workstations and servers called SPINET, along with other smaller security utilities authorized by the Army and designed to probe Unix workstations. Unfortunately, there has not been enough time yet to fully analyze these products and discover all of their capabilities. Until further analysis is completed in this area, scans are made in real-time using the Network General Sniffer and constant reviews are mode of system log files to detect intrusions.

## 2.4 Operational Network Support

*Provide operational computer network systems support. Operational support consists of providing solutions to network problems, collecting information on network status and utilization, and investigating mail distribution problems.*

The Support Center has processed approximately 2500 total help-desk requests during the period of performance of this D.O. This number is very significant when you consider the fact that the Support Center is not advertised as a help desk to the SED community, as well as the group's current staffing level.

Examples of service:

- IP Subnet Maintenance
- Service IP address requests
- Resolve IP address conflicts
- Manage Microsoft Exchange Server User Accounts
- Install and assist with Microsoft Exchange and Microsoft Outlook mail clients
- Assist users with E-mail problems: encoding/decoding attachments, address formats
- Assist with obtaining and configuring dial-in accounts
- Administer and troubleshoot remote connections to the SED LAN
- Install and assist with RATS (Re-engineered Automated Travel System: used for government travel reimbursement.)
- Troubleshoot network connection problems for various user PCs
- Troubleshoot PC, Linux, Mac, Sun, VAX problems, both hardware and software related ("My ... won't work.")
- Installation of network software on various PCs
- Numerous forgotten password problems
- Manage name server entries
- Pathworks Server Maintenance
- Add thin-net ports to offices
- Construct thin-net cables and lay cable in labs and offices
- Insert 10Base-T network drops into offices
- Assist various divisions and projects with the addition of new mail servers to the building net, troubleshoot E-mail routing problems
- Accommodate the network personnel and equipment moves within SED
- Plan for expansion of service team and bolstering of support capabilities

# 3.0 SUMMARY

*Electronic Mail Systems*

Microsoft Exchange is the primary E-mail system in use at SED. The SED Exchange server now has over three hundred users, and handles the load very well. The process of moving the entire user community of the SED continues, though at a slower pace than recently because most users are already migrated. Several upgrades have been performed on the Exchange server during this D.O. These upgrades were done in the continuing effort to achieve greater connectivity and capability for Exchange users, a primary research effort in this D.O. Two connectivity issues were studied: First, how to connect the Exchange server to other Exchange servers on the Redstone Arsenal, and second, how to synchronize the Exchange database with other building databases. Progress was made in both of these areas, but further research is still required. Other areas of research included the impact of DMS on the SED E-Mail system, and possible implementations and capabilities of GroupWare.

*WWW Architecture*

SED employs numerous web sites to assist its users and advertise its presence to the outside world. Currently there is one site for public access and two sites that contain utilities and information pertinent only to users in the SED community. Access to all internal "Intranet" sites is maintained using rules-based security based on a user IP address, and is restricted to be accessible by users within the SED community only. File security on these sites is maintained via the secure nature of OpenVMS, as well as constant vigilance for possible security breaches and possible holes in web security. To date there have been no known problems with security.

Currently Purveyor is in use as a server because of its availability and close tie-in to OpenVMS security, file system architecture and the internal Oracle database. A release of Netscape Enterprise Server for OpenVMS is expected in the future. When this is available it will be inspected for possible use as a substitute for Purveyor.

*Network Traffic Monitoring*

Hub management is being handled Digital Equipment Corporation's (DEC) ClearVISN network management software, a graphical management utility. As DEC equipment is the primary equipment used for backbone transport, ClearVISN is able to handle management of almost all installed equipment.

The Network General Sniffer has proved to be an invaluable tool in monitoring both the Ethernet and FDDI network currently in place at SED. With a possibility of Fast Ethernet in the future, it may be necessary to purchase another Sniffer version capable of Fast Ethernet to add to the tool chest.

Army regulations have been released which address specific requirements and responsibilities regarding network security, as well as tools made available by the Army toward that end. This document was just received and as such has not

been fully analyzed. Full analysis will be addressed in the future when it is complete.

*Operational Network Support*

The Support Center has processed over 2500 total help-desk requests during the period of performance of this D.O. This number is very significant when you consider the fact that the Support Center does not actively advertise its existence to the SED community, as well as the current staffing level. A more accurate total number of requests serviced, along with service times and other typical statistics is difficult to arrive at because not all problems handled were logged electronically. While tracking support calls is an important task, the method in use is currently sufficient. In the future, requirements may arise that would create a recommendation of tracking software for the support team. If and when that need arises, it will be addressed.

## APPENDIX A: Equipment purchased

The following items were purchased on this D.O.:

612TX MultiSwitch Hub 12 UTP Ports 100MBps Fast Ethernet Ports
900TH DecConcentrator 14 UTP Connections DEFHU-MU
VNSwitch 900XX 4100BaseXX Fast Ethernet Ports 3 pack DVNXX-PA
DEFYU-MA: Fast Ethernet Modules for 900XX UTP
DEC Fast Etherworks 10/100 PCI Adapters 5 Pack
20 Microsoft Exchange Client Access Licenses
MS TechNet Unlimited User subscription 1 year
IpSwitch Inc. WS Ping Pro Pack
Norton Utilities for WinNT 10 Pack
Microsoft Exchange Server V5.5 upgrade CD
BP7217 Battery for DSP-100 Cablemeter
LN17X-AA LN17 EP Toner Cartridges
Mic-SC and SC-ST Fiber Cables
Motorola Spirit 2-way Radio
Daisy Chain Connector Kit (8 conn & 1 50ohm term)
DeWalt 12V Flashlight
NT User Administration and NT Quick Reference Book
32 MB Upgrade EDO RAM 72 Pin
SC-SC 3Meter Fiber Cables
Office Supplies